Gigabit Switches

AT-9108
AT-8518
AT-8525
AT-8550

User's Command Guide

Version 4.x

PN 613-10794-00 Rev B

Allied Telesyn

Simply Connecting the World

Copyright © 1999 Allied Telesyn International, Corp.
960 Sewart Drive Suite B, Sunnyvale CA 94086 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn International, Corp.

*Centre*Com is a registered trademark of Allied Telesyn International, Corp.

All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn International, Corp. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn International, Corp. has been advised of, known, or should have known, the possibility of such damages.

Gigabit Switch User's Command Guide

General Switch Commands

Command	Description
clear counters	Clears all switch statistics and port counters.
config account <username> {encrypted} {<password>}	Configures a user account password. Passwords must have a minimum of 4 characters and can have a maximum of 12 characters. User names and passwords are case-sensitive.
config banner	Configures the banner string. You can enter up to 24 rows of 80-column text that is displayed before the login prompt of each session. Press [Return] at the beginning of a line to terminate the command and apply the banner. To clear the banner, press [Return] at the beginning of the first line.
config time <date> <time>	Configures the system date and time. The format is as follows: `mm/dd/yyyy hh:mm:ss` The time uses a 24-hour clock format. You cannot set the year past 2023.
config timezone <GMT_offset> {autodst | noautodst}	Configures the GMT offset and usage of Daylight Savings.The GMT_OFFSET is in +/- minutes from the GMT time. Automatic Daylight Savings Time (DST) changes can be enabled or disabled. The default setting is enabled.
create account [admin | user] <username> {encrypted} {<password>}	Creates a user account. The `encrypted` option should only be used by the switch to generate an ASCII configuration (using the `upload configuration` command), and parsing a switch-generated configuration (using the `download configuration` command).
delete account <username>	Deletes a user account.
disable pace	Disables recognition of the PACE bit. Available only in ingress mode.
enable license [basic_L3 | advanced_L3] <license_key>	Enables a particular software feature license. Specify `<license_key>` as an integer. This command is available only on the AT-8550 and AT-8525. The command `unconfig switch all` does not clear licensing information. This feature cannot be disabled once the license is enabled on the switch.

Command	Description
enable pace	Enables recognition of the PACE bit. Available only in ingress mode.
help	Displays a command summary list.
history	Displays the previous 49 commands entered on the switch.
ping {continuous} {size <n>} [<ip_address> | <hostname>]	Sends ICMP echo messages to a remote IP device. Specify: ❑ `continuous` — ICMP echo messages should be sent continuously. ❑ `size <n>` — The size of the packet. ❑ `ipaddress` — Specifies the IP address of the host. ❑ `hostname` — Specifies the name of the host. To use the `hostname`, you must first configure DNS.
reboot {<date> <time> | cancel}	Reboots the switch at the date and time specified. If you do not specify a reboot time, the reboot happens immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the `cancel` option.
show accounts	Displays the account names, access level, number of successful and failed login attempts, and the number of active sessions in the user database.
show banner	Displays the user-configured banner.
show diag	Displays software diagnostics.
show memory	Displays the current system memory information.
show switch	Displays the current switch information.
show version	Displays the hardware and software versions currently running on the switch.
telnet [<ipaddress> | <hostname>] {<port_number>}	Creates a Telnet session from the current CLI session to another host. If the TCP port number is not specified, port 23 is used. Only VT100 emulation is supported.
traceroute <ipaddress>	Traces the routed path between the switch and a destination endstation.
unconfig switch {all}	Resets all switch parameters (with the exception of defined user accounts) to the factory defaults. If you specify the keyword `all`, the user account information is reset as well.

Network Management and SNMP Commands

Command	Description
clear session <number>	Terminates a Telnet session from the switch.
config snmp add <ipaddress> {<mask>}	Adds the IP address of an SNMP management station to the access list. Up to 32 addresses can be specified.
config snmp add trapreceiver <ipaddress> community <string>	Adds the IP address of a specified trap receiver. The IP address can be a unicast, multicast, or broadcast. A maximum of six trap receivers is allowed.
config snmp community [readonly | readwrite] <string>	Adds an SNMP read or read/write community string. The default `readonly` community string is `public`. The default `readwrite` community string is `private`. Each community string can have a maximum of 126 characters, and can be enclosed by double quotation marks.
config snmp delete [<ipaddress> {<mask>} | all]	Deletes the IP address of a specified SNMP management station or all SNMP management stations. If you delete all addresses, any machine can have SNMP management access to the switch.
config snmp delete trapreceiver [<ip_address> community <string> | all]	Deletes the IP address of a specified trap receiver or all authorized trap receivers.
config snmp syscontact <string>	Configures the name of the system contact. A maximum of 255 characters is allowed.
config snmp syslocation <string>	Configures the location of the switch. A maximum of 255 characters is allowed.
config snmp sysname <string>	Configures the name of the switch. A maximum of 32 characters is allowed. The default sysname is the model name of the device (for example, `9108`). The `sysname` appears in the switch prompt.
disable idletimeout	Disables the timer that disconnects all sessions. Once disabled, console sessions remain open until the switch is rebooted or you logoff. Telnet sessions remain open until you close the Telnet client.
disable rmon	Disables the collection of RMON statistics on the switch.
disable snmp access	Disables SNMP on the switch. Disabling SNMP access does not affect the SNMP configuration (for example, community strings).
disable snmp traps	Prevents SNMP traps from being sent from the switch. Does not clear the SNMP trap receivers that have been configured.
disable telnet	Disables Telnet access to the switch.
disable web	Disables Web access to the switch.
enable idletimeout	Enables a timer that disconnects all sessions (both Telnet and console) after 20 minutes of inactivity. The default setting is disabled.
enable rmon	Enables the collection of RMON statistics on the switch.
enable snmp access	Turns on SNMP support for the switch.
enable snmp traps	Turns on SNMP trap support.
enable telnet	Enables Telnet access to the switch.
enable web	Enables Web access to the switch.
logout | quit	Logs out of a console or Telnet session.

Command	Description
show management	Displays network management configuration and statistics, including enable/disable states for Telnet and SNMP, SNMP community strings, authorized SNMP station list, SNMP trap receiver list, and login statistics.
show session	Displays the currently active Telnet, console, and Web sessions communicating with the switch.
unconfig management	Restores default values to all SNMP-related entries.

VLAN Commands

Command	Description
config dot1p ethertype <ethertype>	Configures an IEEE 802.1Q Ethertype. Use this command only if you have another switch that supports 802.1Q, but uses a different Ethertype value than 8100.
config gvrp {listen | send | both | none} {port <portlist>}	Configures the sending and receiving GVRP information one or all a ports. Options include the following: ❑ `listen` — Receive GVRP packets. ❑ `send` — Send GVRP packets. ❑ `both` — Send and receive GVRP packets. ❑ `none` — Disable the port from participating in GVRP operation. The default setting is `both`.
config protocol <protocol_name> [add | delete] <protocol_type> <hex_value> {<protocol_type> <hex_value>} ...	Configures a protocol filter. Supported <`protocol_type`> values include: ❑ `etype` ❑ llc ❑ snap The variable <`hex_value`> is a hexadecimal number between 0 and FFFF that represents either the Ethernet protocol type (for EtherType), the DSAP/SSAP combination (for LLC), or the SNAP-encoded Ethernet protocol type (for SNAP).
config vlan <name> add port <portlist> {tagged | untagged}	Adds one or more ports to a VLAN. You can specify tagged port(s), untagged port(s). By default, ports are untagged.
config vlan <name> delete port <portlist> {tagged | untagged}	Deletes one or more ports from a VLAN.
config vlan <name> ipaddress <ipaddress> {<mask>}	Assigns an IP address and an optional mask to the VLAN.
config vlan <name> protocol [<protocol_name> | any]	Configures a protocol-based VLAN. If the keyword `any` is specified, then it becomes the default VLAN. All packets that cannot be classified into other protocol-based VLANs are assigned to the default VLAN of that port.
config vlan <name> qosprofile <qosname>	Configures a VLAN to use a particular QoS profile. Dynamic FDB entries associated with the VLAN are flushed once the change is committed.
config vlan <name> tag <vlanid>	Assigns a numerical VLANid. The valid range is from 1 to 4095.
create protocol <protocol_name>	Creates a user-defined protocol.
create vlan <name>	Creates a named VLAN.
delete protocol <protocol>	Removes a protocol.
delete vlan <name>	Removes a VLAN.
disable gvrp	Disables the Generic VLAN Registration Protocol (GVRP).
disable ignore-stp vlan <name>	Allows a VLAN to use STP port information.
enable gvrp	Enables the Generic VLAN Registration Protocol (GVRP). The default setting is disabled.

Command	Description
enable ignore-stp vlan <name>	Enables a VLAN from using STP port information. When enabled, all virtual ports associated with the VLAN are in STP forwarding mode. The default setting is disabled.
show gvrp	Displays the current configuration and status of GVRP.
show protocol {<protocol_name> | all}	Displays protocol-related information.
show vlan {<name> | all>}	When used with the keyword `all`, or with no named VLANs, displays a summary list of VLAN names with a `portlist` and associated status of each. When used with a named identifier, displays port information, including membership list, IP address, and tag information.
unconfig vlan <name> ipaddress	Resets the IP address of the VLAN.

FDB Commands

Command	Description
clear fdb {<mac_address> | vlan <name> | <portlist>}	Clears dynamic FDB entries that match the filter. When no options are specified, the command clears all FDB entries.
config fdb agingtime <number>	Configures the FDB aging time. The range is 15 through 1,000,000 seconds. The default value is 300 seconds. A value of 0 indicates that the entry should never be aged out.
create fdbentry <mac_address> vlan <name> [blackhole | <portlist> | dynamic] {qosprofile <qosname>}	Creates an FDB entry. Specify the following: ❑ `mac_address` — Device MAC address, using colon separated bytes. ❑ `name` — VLAN associated with MAC address. ❑ `blackhole` — Configures the MAC address as a blackhole entry. ❑ `portlist` — Port numbers associated with MAC address. ❑ `dynamic` — Specifies that the entry will be learned dynamically. Used to associated a QoS profile with a dynamically learned entry. ❑ `qosname` — QoS profile associated with MAC address. If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.
delete fdbentry <mac_address> vlan <name>	Deletes a permanent FDB entry.
show fdb {<mac_address> | vlan <name> | <portlist> | permanent | qos}	Displays the switch FDB contents.

Port Commands

Command	Description
config mirroring add [mac <mac_address> | vlan <name> | port <port> | vlan <name> port <portlist>]	Adds a single mirroring filter definition. Up to eight mirroring definitions can be added. You can mirror traffic from a MAC address, a VLAN, a physical port, or a specific VLAN/port combination.
config mirroring delete [mac <mac_address> | vlan <name> | port <port> | vlan <name> port <portlist> | all}	Deletes a particular mirroring filter definition, or all mirroring filter definitions.
config ports <portlist> auto off {speed [10 | 100]} duplex [half | full]	Changes the configuration of a group of ports. Specify the following: ❑ `auto off` — The port will not autonegotiate the settings. ❑ `speed` — The speed of the port (for 10/100 Mbps ports only). ❑ `duplex` — The duplex setting (half- or full-duplex).
config ports <portlist> auto on	Enables autonegotiation for the particular port type; 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.
config ports <portlist> qosprofile <qosname>	Configures one or more ports to use a particular QoS profile.
disable learning port <portlist>	Disables MAC address learning on one or more ports for security purposes. If MAC address learning is disabled, only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded. The default setting is enabled.
disable mirroring	Disables port-mirroring.
disable port <portlist>	Disables a port. Even when disabled, the link is available for diagnostic purposes.
disable sharing <master_port>	Disables a load-sharing group of ports.
disable smartredundancy <portlist>	Disables the smart redundancy feature. If the feature is disabled, the switch changes the active link only when the current active link becomes inoperable.
enable learning port <portlist>	Enables MAC address learning on one or more ports. The default setting is enabled.
enable mirroring to <port>	Dedicates a port to be the mirror output port.
enable port <portlist>	Enables a port.
enable sharing <master_port> grouping <portlist>	Defines a load-sharing group of ports. The ports specified in `<portlist>` are grouped to the master port.
enable smartredundancy <portlist>	Enables the smart redundancy feature on the redundant Gigabit Ethernet port. When the Smart Redundancy feature is enabled, the switch always uses the primary link when the primary link is available. The default setting is enabled.
restart port <portlist>	Resets autonegotiation for one or more ports by resetting the physical link.
show mirroring	Displays the port-mirroring configuration.
show ports {<portlist>} collisions	Displays real-time collision statistics.
show ports {<portlist>} configuration	Displays the port configuration.
show ports {<portlist>} info	Displays detailed system-related information
show ports {<portlist>} packet	Displays a histogram of packet statistics.

Command	Description
show ports {<portlist>} qosmonitor	Displays real-time QoS statistics.
show ports {<portlist>} rxerrors	Displays real-time receive error statistics.
show ports {<portlist>} stats	Displays real-time port statistics.
show ports {<portlist>} txerrors	Displays real-time transmit error statistics.
show ports {<portlist>} utilization	Displays real-time port utilization information. Use the [Spacebar] to toggle between packet, byte, and bandwidth utilization information.
unconfig ports <portlist> display-string <string>	Clears the user-defined display string from a port.

Syslog Commands

Command	Description
clear log {static}	Clears the log. If `static` is specified, the critical log messages are also cleared.
config log display {<priority>}	Configures the real-time log display. Options include: ❑ `priority` — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, error, alert, warning, notice, info, and debug. If not specified, informational priority messages and higher are displayed.
config syslog <ip_address> <facility> {<priority>}	Configures the syslog host address and filters messages sent to the syslog host. Options include: ❑ `ipaddress` — The IP address of the syslog host. ❑ `facility` — The syslog facility level for local use (local0 - local7). ❑ `priority` — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, only critical priority messages and are sent to the syslog host.
disable log display	Disables the log display.
disable syslog	Disables logging to a remote syslog host.
enable log display	Enables the log display.
enable syslog	Enables logging to a remote syslog host.
show log {<priority>}	Displays the current snapshot of the log. Options include: ❑ `priority` — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, informational priority messages and higher are displayed.
show log config	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.

STP Commands

Command	Description
config stpd <stpd_name> add vlan <name>	Adds a VLAN to the STPD.
config stpd <stpd_name> hellotime <value>	Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge. The range is 1 through 10. The default setting is 2 seconds.
config stpd <stpd_name> forwarddelay <value>	Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge. The range is 4 through 30. The default setting is 15 seconds.
config stpd <stpd_name> maxage <value>	Specifies the maximum age of a BPDU in this STPD. The range is 6 through 40. The default setting is 20 seconds. Note that the time must be greater than, or equal to 2 * (Hello Time + 1) and less than, or equal to 2 * (Forward Delay –1).
config stpd <stpd_name> priority <value>	Specifies the priority of the STPD. By changing the priority of the STPD, you can make it more or less likely to become the Root Bridge. The range is 0 through 65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.
config stpd <stpd_name> port cost <value> <portlist>	Specifies the path cost of the port in this STPD. The range is 1 through 65,535. The switch automatically assigns a default path cost based on the speed of the port, as follows: ❑ For a 10Mbps port, the default cost is 100. ❑ For a 100Mbps port, the default cost is 19. ❑ For a 1000Mbps port, the default cost is 4.
config stpd <stpd_name> port priority <value> <portlist>	Specifies the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the Root Port. The range is 0 through 255. The default setting is 128. A setting of 0 indicates the lowest priority.
create stpd <stpd_name>	Creates an STPD. When created, an STPD has the following default parameters: ❑ Bridge priority — 32,768 ❑ Hello time — 2 seconds ❑ Forward delay — 15 seconds
delete stpd <stpd_name>	Removes an STPD. An STPD can only be removed if all VLANs have been deleted from it. The default STPD, s0, cannot be deleted.
disable stpd [<stpd_name> | all]	Disables the STP mechanism on a particular STPD, or for all STPDs.
disable stpd port <portlist>	Disables STP on one or more ports. Disabling STP on one or more ports puts those ports in *forwarding* state; all BPDUs received on those ports will be disregarded.
enable stpd {<stpd_name>}	Enables the STP protocol for one or all STPDs. The default setting is disabled.
enable stpd port {<portlist>}	Enables the STP protocol on one or more ports. If STPD is enabled for a port, Bridge protocol Data Units (BPDUs) will be generated on that port if STP is enabled for the associated STPD. The default setting is enabled.
show stpd {<stpd_name>}	Displays STP information for one or all STPDs on the switch.
show stpd <stpd_name> port <portlist>	Displays port-specific STP information.

Command	Description
unconfig stpd {<stpd_name>}	Restores default STP values to a particular STPD or to all STPDs.

QoS Commands

Command	Description
config ipqos [add | delete] <dest_ipaddress>/<mask_length> [qosprofile <qosname> | blackhole]	Adds or deletes a QoS profile (short form).
config ipqos [add | delete] [tcp | udp | other | all] <ip_dest_addr>/<mask_length> {l4-dstport <tcp/udp_port_number>} {<ip_src_address>/<mask_length>} {l4-srcport <tcp/udp_port_number>} [qosprofile <qosname> | blackhole]	Adds or deletes a QoS profile (long form).
config qosmode [ingress | egress]	Changes the QoS mode to ingress mode or egress mode.
config qosprofile <qosname> {minbw <percent>} {maxbw <percent>} {priority <level>}	Configures a QoS profile. Specify: ❑ `minbw` — The minimum bandwidth percentage guaranteed to be available to this queue. The default setting is 0. ❑ `maxbw` — The maximum bandwidth percentage this queue is permitted to use. The default setting is 100. ❑ `priority` — The service priority for this queue. Settings include low, normal, medium, and high. The default setting is low. Available only in egress mode.
create qosprofile <qosname>	Creates a QoS profile. The default values assigned to a created QoS profile are ❑ Minimum bandwidth — 0% ❑ Maximum bandwidth — 100% ❑ Priority — low
delete qosprofile <qosname>	Deletes a QoS profile.
disable isq vlan <name>	Disables ISQ on a VLAN.
disable qosmonitor	Disables the QoS monitoring capability.
enable isq vlan <name>	Enables ISQ on a per-VLAn basis. If the FDB aging timer is shorter than 3,000 seconds, this command automatically changes the FDB aging timer to 3,000 seconds.
enable qosmonitor {port <port>}	Enables the QoS monitoring capability on the switch. When no port is specified, the QoS monitor automatically samples all the ports. Error messages are logged to the syslog if the traffic exceeds the parameters of the QoS profile(s). The default setting is disabled.
show qosprofile {<qosname>}	Displays QoS profile information.

Access Policy Commands

Command	Description
config access-profile <access_profile> add {vlan <name> | ipaddress <ipaddress> <subnet_mask>	Adds an IP address or VLAN name to the access profile. The entry must be of the same type as the access profile (for example, IP address).
config access-profile <access_profile> delete {vlan <name> | ipaddress <ipaddress> <subnet_mask>	Deletes an IP address or VLAN name from the access profile.
config access-profile <access_profile> mode [permit | deny]	Configures the access profile to be one of the following: ❑ `permit` — Allows the addresses that match the access profile description. ❑ `deny` — Denies the addresses that match the access profile description. The default setting is `permit`.
create access-profile <access_profile> type [vlan | ipaddress]	Creates an access profile. Once the access profile is created, one or more addresses can be added to it, and the profile can be used to control a specific routing protocol
delete access-profile <access_profile>	Deletes an access profile.
show access-profile <access_profile>	Displays access-profile related information for the switch.

Basic IP Commands

Command	Description
config dns-client add <ipaddress>	Adds a DNS name server(s) to the available server list for the DNS client. Up to three name servers can be configured.
config dns-client default-domain <domain_name>	Configures the domain that the DNS client uses if a fully qualified domain name is not entered. For example, if the default domain is configured to be `foo.com`, executing `ping bar` searches for `bar.foo.com`.
config dns-client delete <ipaddress>	Removes a DNS server.
config sntp-client [primary | secondary] server [<ipaddress> | <host_name>]	Configures an NTP server for the switch to obtain time information. Queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the second server.
config sntp-client update-interval <seconds>	Configures the interval between polling for time information from SNTP servers. The default setting is 64 seconds.
config vlan <name> access-profile [<access_profile> | none]	Configures an access policy for VLAN to VLAN traffic on the only.
clear ipfdb {<ipaddress> <netmask> | vlan <name>]	Removes the dynamic entries in the IP forwarding database. If no options are specified, all IP FDB entries are removed.
disable bootp vlan [<name> | all]	Disables the generation and processing of BOOTP packets.
disable ipforwarding {vlan <name>}	Disables routing for one or all VLANs.
disable ipforwarding broadcast {vlan <name>}	Disables routing of broadcasts to other networks.
disable multinetting	Disables IP multinetting on the system.
disable sntp-client	Disables SNTP client functions.
enable bootp vlan [<name> | all]	Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server. The default setting is enabled for all VLANs.
enable ipforwarding {vlan <name>}	Enables IP routing for one or all VLANs. If no argument is provided, enables routing for all VLANs that have been configured with an IP address. The default setting for `ipforwarding` is disabled.
enable ipforwarding broadcast {vlan <name>}	Enables forwarding IP broadcast traffic for one or all VLANs. If no argument is provided, enables broadcast forwarding for all VLANs. To enable, `ipforwarding` must be enabled on the VLAN. The default setting is enabled.
enable multinetting	Enables IP multinetting on the system.
enable sntp-client	Enables Simple Network Time Protocol (SNTP) client functions.
nslookup <hostname>	Displays the IP address of the requested host.
show ipconfig {vlan <name>}	Displays configuration information for one or all VLANs.
show ipfdb {<ipaddress> <netmask> | vlan <name> }	Displays the contents of the IP forwarding database (FDB) table. Used for technical support purposes. If no option is specified, all IP FDB entries are displayed.
show ipfdb {<ipaddress> <mask> | vlan <name> | all}	Displays the contents of the IP forwarding database table.

Command	Description
show ipstats {vlan <name>}	Displays IP statistics for the CPU of the system.
show dns-client	Displays the DNS configuration.
show sntp-client	Displays configuration and statistics associated with SNTP.

BootP, DHCP Proxy, and UDP Profile Commands

Command	Description
config bootprelay add <ipaddress>	Adds the IP destination address to forward BOOTP packets.
config bootprelay delete [<ipaddress> | all]	Removes one or all IP destination addresses for forwarding BOOTP packets.
config udp-profile <profile_name> add <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	Adds a forwarding entry to the specified UDP-forwarding profile name. All broadcast packets sent to `<udp_port>` are forwarded to either the destination IP address (unicast or subnet directed broadcast) or to the specified VLAN as an all-ones broadcast.
config udp-profile <profile-name> delete <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	Deletes a forwarding entry from the specified `udp-profile` name.
config vlan <name> udp-profile <profile_name>	Assigns a UDP-forwarding profile to the source VLAN. Once the UDP profile is associated with the VLAN, the switch picks up any broadcast UDP packets that matches with the user configured UDP port number, and forwards those packets to the user-defined destination. If the UDP port is the DHCP/BOOTP port number, appropriate DHCP/BOOTP proxy functions are invoked.
create udp-profile <profile_name>	Creates a UDP-forwarding profile. You must use a unique name for the UDP-forwarding profile.
delete udp-profile <profile_name>	Deletes a UDP-forwarding profile.
disable bootprelay	Disables the forwarding of BOOTP requests.
enable bootprelay	Enables the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests.
show udp-profile {<profile_name>}	Displays the profile names, input rules of UDP port, destination IP address, or VLAN and the source VLANs to which the profile is applied.
unconfig udp-profile vlan [<name> | all]	Removes the UDP-forwarding profile configuration for one or all VLANs.

IP ARP Commands

Command	Description
config iparp add <ipaddress> <mac_address>	Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.
config iparp delete <ipaddress>	Deletes an entry from the ARP table. Specify the IP address of the entry.
clear iparp {<ipaddress> | vlan <name>}	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
config iparp add proxy <ipaddress> {<mask>} {<mac_address>} {always}	Configures proxy ARP entries. Up to 64 proxy ARP entries can be configured. When `mask` is not specified, an address with the mask 255.255.255.255 is assumed. When `mac_address` is not specified, the MAC address of the switch is used in the ARP Response. When `always` is specified, the switch answers ARP Requests without filtering requests that belong to the same subnet of the receiving router interface.
config iparp delete proxy [<ipaddress> {<mask>} | all]	Deletes one or all proxy ARP entries.
config iparp timeout <minutes>	Configures the IP ARP timeout period. The default setting is 20 minutes. A setting of 0 disables ARP aging.
show iparp {<ipaddress | vlan <name> | permanent}	Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, VLAN, or permanent entries.
show iparp proxy {<ipaddress> {<mask>}}	Displays the proxy ARP table.

IP Route Commands

Command	Description
config iproute add <ipaddress> <mask> <gateway> <metric>	Adds a static address to the routing table. Use a value of 255.255.255.255 for `mask` to indicate a host entry
config iproute add blackhole <ipaddress> <mask>	Adds a `blackhole` address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.
config iproute add default <gateway> {<metric>}	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface. If no metric is specified, the default metric of 1 is used.
config iproute delete <ipaddress> <mask> <gateway>	Deletes a static address from the routing table.
config iproute delete blackhole <ipaddress> <mask>	Deletes a `blackhole` address from the routing table.
config iproute delete default <gateway>	Deletes a default gateway from the routing table.
config iproute priority [rip | bootp | icmp | static | ospf-intra | ospf-inter | ospf-as-external | ospf-extern1 | ospf-extern2] <priority>	Changes the priority for all routes from a particular route origin.
disable iproute sharing	Disables load sharing for multiple routes.
enable iproute sharing	Enables load sharing if multiple routes to the same destination are available. Only paths with the same lowest cost are shared. The default setting is enabled.
show ipqos {<ip_destination_address> <mask>}	Displays the IP QoS table.
show iproute {priority | vlan <name> | permanent | <ipaddress> <mask>}	Displays the contents of the IP routing table.

ICMP Commands

Command	Description
config irdp <mininterval> <maxinterval> <lifetime> <preference>	Configures the router advertisement message timers, using seconds. Specify: ❑ `mininterval` — The minimum amount of time between router advertisements. The default setting is 450 seconds. ❑ `maxinterval` — The maximum time between router advertisements. The default setting is 600 seconds. ❑ `lifetime` — The default setting is 1,800 seconds. ❑ `preference` — The preference level of the router. An ICMP Router Discover Protocol (IRDP) client always uses the router with the highest preference level. Change this setting to encourage or discourage the use of this router. The default setting is 0.
config irdp [multicast | broadcast]	Configures the destination address of the router advertisement messages. The default setting is `multicast`.
disable icmp redirects {vlan <name>}	Disables the generation of ICMP redirects on one or all VLANs.
disable icmp unreachables {vlan <name>}	Disables the generation of ICMP unreachable messages on one or all VLANs.
disable icmp useredirects	Disables the changing of routing table information when an ICMP redirect message is received.
disable irdp {vlan <name>}	Disables the generation of router advertisement messages on one or all VLANs.
enable icmp redirects {vlan <name>}	Enables generation of ICMP redirect messages on one or all VLANs. The default setting is enabled.
enable icmp unreachables {vlan <name>}	Enables the generation of ICMP unreachable messages on one or all VLANs. The default setting is enabled.
enable icmp useredirects	Enables the modification of route table information when an ICMP redirect message is received. The default setting is disabled.
enable irdp {vlan <name>}	Enables the generation of ICMP router advertisement messages on one or all VLANs. The default setting is enabled.
unconfig icmp	Resets all ICMP settings to the default values.
unconfig irdp	Resets all router advertisement settings to the default values.

IP RIP Commands

Command	Description
config rip add vlan [<name> | all]	Configures RIP on an IP interface. If no VLAN is specified, then `all` is assumed. When an IP interface is created, per-interface RIP configuration is disabled by default.
config rip delete vlan [<name> | all]	Disables RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
config rip garbagetime {<delay>}	Configures the RIP garbage time. The timer granularity is 10 seconds. The default setting is 120 seconds.
config rip routetimeout {<delay>}	Configures the route timeout. The timer granularity is 10 seconds. The default setting is 180 seconds.
config rip rxmode [none | v1only | v2only | any] {vlan <name>}	Changes the RIP receive mode for one or all VLANs. Specify: ❑ `none` — Drop all received RIP packets. ❑ `v1only` — Accept only RIP v1 format packets. ❑ `v2only` — Accept only RIP v2 format packets. ❑ `any` — Accept both RIP v1 and v2 packets. If no VLAN is specified, the setting is applied to all VLANs. The default setting is `any`.
config rip txmode [none | v1only | v1comp | v2only] {vlan <name>}	Changes the RIP transmission mode for one or all VLANs. Specify: ❑ `none` — Do not transmit any packets on this interface. ❑ `v1only` — Transmit RIP v1 format packets to the broadcast address. ❑ `v1comp` — Transmit RIP v2 format packets to the broadcast address. ❑ `v2only` — Transmit RIP v2 format packets to the RIP multicast address. If no VLAN is specified, the setting is applied to all VLANs. The default setting is `v2only`.
config rip updatetime {<delay>}	Changes the periodic RIP update timer. The timer granularity is 10 seconds. The default setting is 30 seconds.
config rip vlan [<name> | all] export-filter [<access-profile> | none]	Configures RIP to suppress certain routes when performing route advertisements.
config rip vlan [<name> | all] import-filter [<access_profile> | none]	Configures RIP to ignore certain routes received from its neighbor.
config rip vlan [<name> | all] trusted-gateway [<access_profile> | none]	Configures RIP to use the access list to determine which RIP neighbor to receive (or reject) the routes.
disable rip	Disables RIP.
disable rip aggregation	Disables the RIP aggregation of subnet information on a RIP v2 interface.
disable rip export osfp	Disables the distribution of OSPF routes into the RIP domain.
disable rip export static	Disables the filtering of static routes.
disable rip poisonreverse	Disables poison reverse.
disable rip splithorizon	Disables split horizon.
disable rip triggerupdate	Disables triggered updates.
enable rip	Enables RIP. The default setting is disabled.

Command	Description
show rip stat {vlan <name>}	Displays RIP-specific statistics for one or all VLANs.
unconfig rip {vlan <name>}	Resets all RIP parameters to match the default VLAN. Does not change the enable/disable state of the RIP settings. If no VLAN is specified, all VLANs are reset.
enable rip aggregation	Enables RIP aggregation of subnet information an interface configured to sent RIP v2 or RIP v2-compatible traffic.The following rules apply when using RIP aggregation: ❑ Subnet routes are aggregated to the nearest class network route when crossing a class boundary. ❑ Within a class boundary, no routes are aggregated. ❑ If aggregation is enabled, the behavior is the same as in RIP v1. ❑ If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary. The default setting is disabled.
enable rip export static	Enables the advertisement of static routes using RIP. The default setting is disabled.
enable rip poisonreverse	Enables the split horizon with poison-reverse algorithm for RIP. The default setting is enabled. If you enable poison reverse and split horizon, poison reverse takes precedence.
enable rip splithorizon	Enables the split horizon algorithm for RIP. Default setting is enabled.
enable rip triggerupdate	Enables triggered updates. *Triggered updates* are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
show rip {vlan <name>}	Displays RIP configuration and statistics for one or all VLANs.

IP OSPF Commands

Command	Description
config ospf add virtual-link <routerid> <areaid>	Adds a virtual link connected to another ABR. Specify the following: ❑ `routerid` — Far-end router interface number. ❑ `areaid` — Transit area used for connecting the two end-points. The transit area cannot have the IP address 0.0.0.0.
config ospf add vlan [<name> | all]	Enables OSPF on one or all VLANs (router interfaces). The default setting is disabled.
config ospf area <areaid> add range <ipaddress> <mask> [advertise | noadvertise] {type 3 | type 7}	Configures a range of IP addresses in an OSPF area. If advertised, the range is exported as a single LSA by the ABR.
config ospf area <areaid> delete range <ipaddress> <mask>	Deletes a range of IP addresses in an OSPF area.
config ospf area <area_id> external-filter [<access_profile> | none]	Configures the router to use the access policy to determine which external routes are allowed to be exported into the area. This router must be an ABR.
config ospf area <area_id> interarea-filter [<access_profile> | none]	Configures the router to use the access policy to determine which inter-area routes are allowed to be exported into the area. This router must be an ABR.
config ospf area <areaid> normal	Configures an OSFP area as a normal area. The default setting is `normal`.
config ospf area <areaid> nssa [summary | nosummary] stub-default-cost <cost> {translate}	Configures an OSPF area as a NSSA.
config ospf area <areaid> stub [summary | nosummary] stub-default-cost <cost>	Configures an OSPF area as a stub area.
config ospf asbr-filter [<access_policy> | none]	Configures a route filter for all the routes OSPF exports from RIP or other sources.
config ospf [vlan <name> | area <areaid> | virtual-link <routerid> <areaid>] authentication [simple-password <password> | md5 <md5_key_id> <md5_key>| none]	Specifies the authentication password (up to eight characters) or Message Digest 5 (MD5) key for one or all interfaces in an area. The `md5_key` is a numeric value with the range 0 to 65,536. When the OSPF area is specified, authentication information is applied to all OSPF interfaces within the area.
config ospf [area <areaid> | vlan [<name> | all]] cost <number>	Configures the cost metric of one or all interface(s). The default cost is 1.
config ospf delete virtual-link <routerid> <areaid>	Removes a virtual link.
config ospf delete vlan [<name> | all]	Disables OSPF on one or all VLANs (router interfaces).
config ospf [area <areaid> | vlan [<name> | all]] priority <number>	Configures the priority used in the designated router-election algorithm for one or all IP interface(s) of for all the interfaces within the area. The range is 0 through 255, and the default setting is 1. Setting the value to 0 ensures that the router is never selected as the designated router or backup designated router.
config ospf routerid [automatic | <routerid>]	Configures the OSPF router ID. If automatic is specified, the switch uses the largest IP interface address as the OSPF router ID. The default setting is `automatic`.

Command	Description
config ospf spf-hold-time {<seconds>}	Configures the minimum number of seconds between Shortest Path First (SPF) recalculations. The default setting is 3 seconds.
config ospf spf-hold-time {<seconds>}	Configures the minimum number of seconds between Shortest Path First recalculations. The default setting is 3 seconds.
config ospf [vlan <name> | area <areaid> | virtual-link <routerid>] timer <retransmission_interval> <transmission_delay> <hello_interval> <dead_interval>	Configures the timers for one interface or all interfaces in the same OSPF area. The following default, minimum, and maximum values (in seconds) are used: ❑ `retransmission_interval` Default: 5 Minimum: 0 Maximum: 3,600 ❑ `transmission_delay` Default: 1 Minimum: 0 Maximum: 3,600 ❑ `hello _interval` Default: 10 Minimum: 1 Maximum: 65,535 ❑ `dead_interval` Default: 40 Minimum: 1 Maximum: 2,147,483,647
config ospf [vlan <name> | area <areaid> | virtual-link <routerid>] timer <retransmission_interval> <transmission_delay> <hello_interval> <dead_interval>	Configures the timers for one interface or all interfaces in the same OSPF area. The following default, minimum, and maximum values (in seconds) are used: ❑ `retransmission_interval` Default: 5 Minimum: 0 Maximum: 3600 ❑ `transmission_delay` Default: 1 Minimum: 0 Maximum: 3600 ❑ `hello _interval` Default: 10 Minimum: 1 Maximum: 65535 ❑ `dead_interval` Default: 40 Minimum: 1 Maximum: 2147483647
config ospf vlan <name> area <areaid>	Associates a VLAN (router interface) with an OSPF area. All router interfaces must have an associated OSPF area. By default, all router interfaces are associated with area 0.0.0.0.
create ospf area <areaid>	Creates an OSPF area. Area 0.0.0.0 does not need to be created. It exists by default.

Command	Description
delete ospf area [<areaid> | all]	Deletes and OSPF area. Once an OSPF area is removed, the associated OSPF area and OSPF interface information is removed.
disable ospf	Disables OSPF.
disable ospf export rip	Disables exporting of RIP routes to other OSPF routers.
disable ospf export static	Disables exporting of statically configured routes.
enable ospf	Enables OSPF process for the router.
enable ospf export rip cost {<metric>} [ase-type-1 | ase-type-2] {tag <number>}	Enables the distribution of RIP routes into the OSPF domain. The default tag number is 0. The default setting is disabled.
enable ospf export static cost {<metric>} [ase-type-1 | ase-type-2] {tag <number>}	Enables the distribution of static routes into the OSPF domain. The default tag number is 0. The default setting is disabled.
show ospf	Displays global OSPF information.
show ospf area {<areaid>}	Displays information about a particular OSPF area, or all OSPF areas.
show ospf interfaces {vlan <name> | area <areaid>}	Displays information about one or all OSPF interfaces. If no argument is specified, all OSPF interfaces are displayed.
show ospf lsdb {detail} area [<areaid> | all] [router | network | summary-net | summary-asb | as-external | external-type7 |all]	Displays a table of the current LSDB. You can filter the display using either the area ID, the remote router ID, or the link-state ID. The default setting is `all` with no detail. If `detail` is specified, each entry includes complete LSA information.
show ospf virtual-link {<areaid> <routerid> }	Displays virtual link information about a particular router or all routers.
unconfig ospf {vlan <name> | area <areaid>}	Resets one or all OSPF interfaces to the default settings.

IP Multicast Commands

Command	Description
clear igmp snooping {vlan <name>}	Removes one or all IGMP snooping entries.
clear ipmc cache {<group> {<src_ipaddress> <mask>}}	Resets the IP multicast cache table. If no options are specified, all IP multicast cache entries are flushed.
config igmp <query_interval> <query_response_interval> <last_member_query_interval>	Configures the IGMP timers. Timers are based on RFC2236. Specify the following: ❑ `query_interval` — The amount of time, in seconds, the system waits between sending out General Queries. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 125 seconds. ❑ `query_response_interval` — The maximum response time inserted into the periodic General Queries. The range is 1 to 25 seconds. The default setting is 10 seconds. ❑ `last_member_query_interval` — The maximum response time inserted into a Group-Specific Query sent in response to a Leave group message. The range is 1 to 25 seconds. The default setting is 1 second.
config igmp snooping <router_timeout> <host_timeout>	Configures the IGMP snooping timers. Timers should be set to approximately 2.5 times the router query interval in use on the network. Specify the following: ❑ `router_timeout` — The interval, in seconds, between the last time the router was discovered and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds. ❑ `host_timeout` — The interval, in seconds, between the last IGMP group report message from the host and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.
disable igmp {vlan <name>}	Disables the router-side IGMP processing on a router interface. No IGMP query is generated, but the switch continues to respond to IGMP queries received from other devices. If no VLAN is specified, IGMP is disabled on all router interfaces.
disable igmp snooping	Disables IGMP snooping. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given VLAN.
disable ipmcforwarding {vlan <name> | all}	Disables IP multicast forwarding.
enable igmp {vlan <name> | all}	Enables IGMP on a router interface. The default setting is enabled.
enable igmp snooping {vlan <name> | all}	Enables IGMP snooping. The default setting is disabled.
show ipmc cache {<group> {<src_ipaddress> <mask>}} | all}	Displays the IP multicast forwarding cache.
disable ipmcforwarding {vlan <name>}	Disables IP multicast forwarding.
show igmp snooping {<vlan <name>}	Displays IGMP snooping registration information, and a summary of all IGMP timers and states.
show ipmc cache {detail} {<group> {<src_ipaddress> <mask>}}	Displays the IP multicast forwarding cache.

Command	Description
unconfig igmp	Resets all IGMP settings to their default values and clears the IGMP group table.

DVMRP Commands

Command	Description
config dvmrp add vlan [<name> | all]	Enables DVMRP one or all IP interfaces. If no VLAN is specified, DVMRP is enabled on all IP interfaces. When an IP interface is created, DVMRP is disabled by default.
config dvmrp delete vlan [<name> | all]	Disables DVMRP on one or all IP interfaces. If no VLAN is specified, DVMRP is disabled on all IP interfaces.
config dvmrp timer <route_report_interval> <route_replacement_time>	Configures the global DVMRP timers. Specify the following: ❑ `route_report_interval` — The amount of time the system waits between transmitting periodic route report packets. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 60 seconds. Because triggered update is always enabled, the route report will always be transmitted prior to the expiration of the route report interval. ❑ `route_replacement_time` — The hold-down time before a new route is learned, once the previous route has been deleted. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 140 seconds.
config dvmrp vlan [<name> | all] export-filter [<access_profile> | none]	Configures DVMRP to filter out certain routes when performing the route advertisement.
config dvmrp vlan [<name> | all] import-filter [<access_profile> | none]	Configures DVMRP to filter certain routes received from its neighbor.
config dvmrp vlan [<name> | all] trusted-gateway [<access_profile> | none]	Configures DVMRP to use the access policy to determine which DVMRP neighbor is trusted and to receive routes from.
config dvmrp vlan <name> timer <probe_interval> <neighbor_timeout_interval>	Configures DVMRP interface timers. Specify the following: ❑ `probe_interval` — The amount of time that the system waits between transmitting DVMRP probe messages. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 10 seconds. ❑ `neighbor_timeout_interval` — The amount of time before a DVMRP neighbor route is declared to be down. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 35 seconds.
disable dvmrp	Disables DVMRP on the system.
enable dvmrp	Enables DVMRP on the system. The default setting is disabled.
show dvmrp {vlan <name> | route}} {detail}	Displays the DVMRP configuration and statistics, or the unicast route table. The default setting is all.
unconfig dvmrp {vlan <name>}	Resets the DVMRP timers to their default settings. If no VLAN is specified, all interfaces are reset.

PIM-DM Commands

Command	Description
config pim-dm add vlan [<name> | all]	Enables PIM-DM on an IP interface. When an IP interface is created, per-interface PIM-DM configuration is disabled by default.
config pim-dm delete vlan [<name> | all]	Disables PIM-DM on an interface.
config pim-dm timer <hello_interval>	Configures the global PIM-DM timers. Specify the following: ❑ `hello_interval` — The amount of time before a hello message is sent out by the PIM-DM router. The range is 1 to 65,519 seconds. The default setting is 30 seconds.
config pim-dm vlan [<name> | all] trusted-gateway [<access-profile> | none]	Configures PIM-DM to use the access profile to determine which PIM-DM neighbor is to receive or reject the routes.
disable pim-dm	Disables PIM-DM on the system.
enable pim-dm	Enables PIM-DM on the system. The default setting is disabled.
show pim-dm {vlan <name>}	Displays the PIM-DM configuration and statistics. If no VLAN is specified, the configuration is displayed for all PIM-DM interfaces.
unconfig pim-dm {vlan <name>}	Resets all PIM-DM settings to their default values.

IPX Commands

Command	Description
config ipxmaxhops <number>	Configures the IPX maximum hop count when forwarding IPX packets. The default setting is 16. Change this only if NetWare Lin Services Protocol (NLSP) is running in the IPX network.
config ipxroute add [<dest_netid> | default] <next_hop_id> <next_hop_node_addr> <hops> <tics>	Adds a static IPX route entry in the IPX route table. Specify: ❑ `next_hop_id` — The NetID of the neighbor IPX network. ❑ `next_hop_node_addr` — The node address of the next IPX router. ❑ `hops` — The maximum hop count. ❑ `tics` — The timer delay value. Up to 64 static routes can be entered.
config ipxroute delete [<dest_netid> | default] <next_hope_netid> <next_hope_node_addr>	Removes a static IPX route entry from the route table.
config ipxservice add <service_type> <service_name> <netid> <mac_address> <socket> <hops>	Adds a static entry to the IPX service table. Specify: ❑ `service_type` — The service type. ❑ `service_name` — The service name. ❑ `netid` — The IPX network identifier of the server. ❑ `mac_address` — The MAC address of the server. ❑ `socket` — The IPX port number on the server. ❑ `hops` — The number of hops (for SAP routing purposes).
config ipxservice delete <service_type> <service_name> <netid> <mac_address> <socket>	Deletes an IPX service from the service table.
config vlan <name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 | enet_snap]	Configures a VLAN to run IPX routing. Specify: ❑ `enet_ii` — Uses standard Ethernet 2 header. ❑ `enet_8023` — Uses IEEE 802.3 length field, but does not include the IEEE 802.2 LLC header. ❑ `enet_8022` — Uses standard IEEE format and uses IEEE 802.2 LLC header. ❑ `enet_snap` — Adds Subnetwork Access Protocol (SNAP) header to IEEE 802.2 LLC header.
disable type20 forwarding {vlan <name>}	Disables the forwarding of IPX type 20 packets.
enable type20 forwarding {vlan <name>}	Enables the forwarding of IPX type 20 (NetBIOS inside IPX) packets from one or more ingress VLANs. The default setting is disabled.
show ipxconfig {vlan <name>}	Displays IPX configuration information for one or all VLANs.
show ipxroute {vlan <name> | xnetid <netid> | origin [static | rip | local]}	Displays the IPX routes in the route table.
show ipxservice {vlan <name> | xnetid <netid> | origin [static | sap | local]}	Displays IPX services learned by way of SAP.
show ipxstats {vlan <name>}	Displays IPX packet statistics for the IPX router, and one or all VLANs.
unconfig vlan <name> xnetid	Removes the IPX NetID of a VLAN.
xping {continuous} {size <n>} <netid> <mac_address>	Pings an IPX node. If `continuous` is not specified, 4 pings are sent. The default ping packet size is 256 data bytes. The size between 1 and 1,484 bytes.

IPX/RIP Commands

Command	Description
config ipxrip add vlan [<name> | all}	Configures one or all IPX VLANs to run IPX/RIP. IPX/RIP is enabled by default when you configure the IPX VLAN.
config ipxrip delete vlan [<name> | all]	Disables IPX/RIP on one or all interfaces.
config ipxrip {vlan <name> | all} max-packet-size <number>	Configures the maximum transmission unit (MTU) size of the IPX/RIP packet. the default setting is 432 bytes.
config ipxrip vlan [<name> | all] update-interval <time> {hold-multiplier <number>}	Configures the update interval and hold multiplier for IPX/RIP updates. This setting affects both the periodic update interval of IPX/RIP and the aging interval of learned routes. The default update interval is 60 seconds. The aging period is calculated using the formula (update-interval * multiplier). The default multiplier is 3.
config ipxrip vlan [<name> | all] delay <msec>	Configures the time between each IPX/RIP packet within an update interval. The default setting is 55 milliseconds.
disable ipxrip	Disables IPX/RIP on the router.
enable ipxrip	Enables IPX/RIP on the router.
show ipxrip {vlan <name>}	Displays IPX/RIP configuration and statistics for one or all VLANs.
unconfig ipxrip {vlan <name>}	Resets the IPX/RIP settings on one or all VLANs to the default. Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

IPX/SAP Commands

Command	Description
config ipxsap add vlan [<name> | all]	Configures an IPX VLAN to run IPX/SAP routing. If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.
config ipxsap delete vlan [<name> | all]	Disables IPX/SAP on an interface.
config ipxsap vlan [<name> | all] delay <msec>	Configures the time between each SAP packet within an update interval. The default setting is 55 milliseconds.
config ipxsap vlan <name> gns-delay <msec>	Configures the amount of time the switch waits before answering a GNS request. By default, the switch answers a GNS request as soon as possible (0 milliseconds).
config ipxsap vlan [<name> | all] max-packet-size <number>	Configures the MTU size of the IPX/SAp packets. The default setting is 432 bytes.
config ipxsap vlan [<name> | all] update-interval <time> {hold-multiplier <number>}	Configures the update interval and hold multiplier for IPX/SAP updates. This setting affects both the periodic update interval of SAP and the aging interval of learned routes. The default update interval is 60 seconds. The aging period is calculated using the formula (update-interval * multiplier). The default multiplier is 3. Triggered update is always enabled; therefore, new information is processed and propagated immediately.
disable ipxsap	Disables IPX/SAP on the router.
disable ipxsap gns-reply {vlan <name>}	Disables GNS reply on one or all IPX interfaces.
enable ipxsap	Enables IPX/SAP on the router.
enable ipxsap gns-reply {vlan <name>}	Enables GNS reply on one or all IPX interfaces. If no VLAN is specified, GNS reply is enabled on all IPX interfaces. The default setting is enabled.
show ipxsap {vlan <name>	Displays IPX/SAP configuration and status for one or all VLANs.
unconfig ipxsap {vlan <name>}	Resets the IPX/SAP settings on one or all VLANs to the default. Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

Configuration and Image Commands

Command	Description
download bootrom <ipaddress> <filename>	Downloads a BOOT ROM image from a TFTP server. The downloaded image replaces the BOOT ROM in the onboard FLASH memory. Note: If this command does not complete successfully it could prevent the switch from booting.
download config <ipaddress> <filename>	Downloads a previously saved ASCII configuration file from a specific IP host.
download image [xmodem | [<ipaddress> | <hostname>] <filename>] {primary | secondary}	Downloads a new image by way of XMODEM using the serial port, or from a TFTP server over the network. If no parameters are specified, the image is saved to the current image. XMODEM is not supported over a Telnet session.
reboot {<date> <time> | cancel}	Reboots the switch at the date and time specified. If you do not specify a reboot time, the reboot happens immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the `cancel` option.
save {configuration} {primary | secondary}	Saves the current configuration to nonvolatile storage. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the primary configuration area.
show configuration	Displays the current configuration to the terminal. You can then capture the output and store it as a file.
upload config [<ipaddress> | <hostname>] <filename> {every <time> | cancel}	Uploads the current run-time configuration to the specified TFTP server. If `every <time>` is specified, the switch automatically saves the configuration to the server once per day, at the specified time. To cancel automatic upload, use the `cancel` option. If no options are specified, the current configuration is uploaded immediately.
use configuration [primary | secondary]	Configures the switch to use a particular configuration on the next reboot. Options include the primary configuration area or the secondary configuration area.
use image [primary | secondary]	Configures the switch to use a particular image on the next reboot.